REMARKS

Claims 1-5, 7-13, 15-20 and 22-26 were pending and stand rejected. Claims 1, 9, 16 and 23 have been amended. Claims 1-5, 7-13, 15-20 and 22-26 are pending upon entry of this amendment.

Claims 1-3, 5, 7-11, 13, 15-18, 20 and 22-26 were rejected under 35 USC § 103(a) as allegedly being unpatentable over Porras et al. (U.S. Patent No. 6,704,874) ("Porras") and further in view of Pifer et al. (U.S. Patent No. 4,914,444) ("Pifer") and Halstead, Jr. et al. (U.S. Patent No. 5,896,524) ("Halstead"). Applicant respectfully traverses in view of the amended claims.

As amended, claim 1 recites in part (emphasis added):

determine, based on the first alert and the second alert, whether the first clock and the second clock are synchronized; and
if the first clock and the second clock are not synchronized:
synchronize the first clock and the second clock;
modify at least one of a timestamp within the first alert and a timestamp within the second alert; and
after having modified at least one of the timestamp within the first alert and the timestamp within the second alert, determine whether the first alert and the second alert satisfy a condition of a rule, wherein the rule determines whether a security incident has occurred.

As described in the pending application, the claimed invention comprises a first software agent, a second software agent, and a manager module (¶¶12-15; FIG. 1). The manager module receives a first stream of alerts from a first network security device having a first clock and a second stream of alerts from a second network security device having a second clock (¶22). The manager module identifies a first alert in the first stream and a second alert in the second stream, wherein the first alert includes an Internet Protocol (IP) address, and wherein the second alert

includes the IP address (¶¶23-24). The manager module determines, based on the first alert and the second alert, whether the first clock and the second clock are synchronized (¶26). If the first clock and the second clock are not synchronized, the manager module synchronizes the first clock and the second clock (¶26), modifies at least one of a timestamp within the first alert and a timestamp within the second alert (¶36), and after timestamp modification, determines whether the first alert and the second alert satisfy a condition of a rule (¶17), where the rule determines whether a security incident has occurred (¶15).

In one embodiment, a manager module uses a rules engine to determine whether the first alert and the second alert satisfy a condition of a rule (¶¶14-15, 17; FIG. 1), and the rule determines whether a security incident has occurred (¶15). For example, one rule may be that if twenty or more unsuccessful logins are followed by a successful login from the same IP address, then a security incident representing a successful brute force dictionary attack has occurred (¶15 and ¶17).

A rule can be time-sensitive (¶18). For example, the rule above can be modified to require that the twenty or more unsuccessful logins occur within a one minute time period (¶18). If the login events include incorrect timestamps due to the clocks not being synchronized, the rule will not work as intended (¶21). Thus, in order to solve this problem, if the first clock and the second clock are not synchronized, at least one of a timestamp within the first alert and a timestamp within the second alert will be modified before determining whether the first alert and the second alert satisfy a condition of a rule (¶21).

Applicant agrees with the Examiner that Porras does not disclose, teach, or suggest "if the first clock and the second clock are not synchronized: … correlate the first alert and the second alert according to a rule, which comprises determining whether the first alert and the

second alert satisfy a condition of the rule" (Detailed Action, page 3). It follows that Porras does not disclose, teach, or suggest "if the first clock and the second clock are not synchronized: … after having modified at least one of the timestamp within the first alert and the timestamp within the second alert, determine whether the first alert and the second alert satisfy a condition of a rule, wherein the rule determines whether a security incident has occurred."

Similarly, Halstead does not disclose, teach, or suggest the claimed element described above. Halstead discloses determining a global time base from the local clocks' data in a multiprocessor system (abstract). In Halstead, after the time stamps of events in a global event log have been modified, the modified data is simply stored.

Pifer does not remedy this deficiency. Specifically, Pifer does not disclose, teach, or suggest the claimed element "if the first clock and the second clock are not synchronized: … after having modified at least one of the timestamp within the first alert and the timestamp within the second alert, determine whether the first alert and the second alert satisfy a condition of a rule, wherein the rule determines whether a security incident has occurred."

Claim 1 (as amended) recites "determine whether the first alert and the second alert satisfy a condition of a rule, wherein the rule determines whether a security incident has occurred." On January 6, 2009, the Examiner and Applicant's representatives (Sabra-Anne Truesdale, Reg. No. 55,687, and Fengling Li, Reg. No. 62,962) had a telephone conversation during which Applicant's representative (Sabra-Anne Truesdale) explained to the Examiner that Pifer does not disclose, teach, or suggest this element recited in claim 1 (as amended). The Examiner agreed with Applicant's representatives, and the Examiner further stated that Porras, Pifer, and Halstead, both individually and in combination, do not disclose, teach, or suggest the claimed element.

Therefore, claim 1 is patentable over Porras, Pifer, and Halstead, both individually and in combination. Independent claims 9, 16, and 23 (as amended) recite similar language and are also patentable over Porras, Pifer, and Halstead, both individually and in combination, for at least the same reasons.

Claims 4, 12, and 19 were rejected under 35 USC 103(a) as being unpatentable over Porras in view of Pifer, Halstead, and Apel et al. (U.S. Patent No. 6,760,687) ("Apel"). Applicant respectfully traverses. For the record, Applicant also traverses the Examiner's assertions regarding the disclosure of Apel and regarding the motivation to combine Porras, Pifer, Halstead, and Apel.

The claims not specifically mentioned above depend from claims 1, 9, 16, or 23 (directly or indirectly), which were shown to be patentable over Porras in view of Pifer and Halstead. In addition, these claims recite other features not included in claims 1, 9, 16, or 23. Thus, these claims are patentable over Porras in view of Pifer and Halstead, for at least the reasons discussed above, as well as for the elements that they individually recite.

Applicant respectfully submits that the pending claims are allowable over the cited art of record and requests that the Examiner allow this case. The Examiner is invited to contact the undersigned in order to advance the prosecution of this application.

Respectfully submitted,
HUGH S. NJEMANZE

Dated: January 8, 2009 By: /Fengling Li/

Fengling Li, Patent Agent
Reg. No. 62,962
Fenwick & West LLP
Silicon Valley Center
801 California Street
Mountain View, CA 94041
Tel. (650) 335-7182
Fax (650) 938-5200